

On the Rate of Channel Polarization

Erdal Arıkan

Department of Electrical-Electronics Engineering
Bilkent University
Ankara, TR-06800, Turkey
Email: arikan@ee.bilkent.edu.tr

Emre Telatar

Information Theory Laboratory
Ecole Polytechnique Fédérale de Lausanne
CH-1015 Lausanne, Switzerland
Email: emre.telatar@epfl.ch

Abstract—It is shown that for any binary-input discrete memoryless channel W with symmetric capacity $I(W)$ and any rate $R < I(W)$, the probability of block decoding error for polar coding under successive cancellation decoding satisfies $P_e \leq 2^{-N^\beta}$ for any $\beta < \frac{1}{2}$ when the block-length N is large enough.

I. INTRODUCTION

Channel polarization is a method, introduced in [1], for constructing a class of capacity-achieving codes, called *polar codes*, on binary-input symmetric channels. Polar codes are of interest theoretically because they have a well-defined construction rule (that involves no trial-and-error) and are *provably* capacity-achieving. The aim of this paper is to strengthen the results of [1] on the probability of block decoding error for polar codes. We begin by giving the notation and the general problem set-up.

Let $W : \mathcal{X} \rightarrow \mathcal{Y}$ be an arbitrary binary-input DMC (B-DMC) with input alphabet $\mathcal{X} = \{0, 1\}$, output alphabet \mathcal{Y} , and transition probabilities $\{W(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$. Let $I(W)$ denote the *symmetric capacity* of W defined as the mutual information (in bits) between the input and output terminals of W when the input is chosen from the uniform distribution on \mathcal{X} . This parameter takes values in $[0, 1]$ and sets a limit on achievable rates across the channel W using codes that employ the channel input letters with equal frequency. Let $Z(W) = \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}$. This parameter also takes values in $[0, 1]$ and is an upper bound on the probability of ML decision error when the channel is used only once to transmit either a 0 or a 1. We will use $Z(W)$ as a measure of reliability.

The parameter $I(W)$ is of a more fundamental nature than $Z(W)$, however, $Z(W)$ will play a more central role in the following analysis since it is more readily tractable. A useful pair of inequalities that relate these two parameters are

$$\begin{aligned} I(W)^2 + Z(W)^2 &\leq 1, \\ I(W) + Z(W) &\geq 1, \end{aligned} \tag{1}$$

both proved in [1].

A. A channel transform

Let \mathcal{W} denote the class of all B-DMCs as defined above. Consider a channel transform $W \mapsto (W^-, W^+)$ that maps \mathcal{W} to \mathcal{W}^2 . Suppose the transform operates on an input channel

$W : \mathcal{X} \rightarrow \mathcal{Y}$ to generate the channels $W^- : \mathcal{X} \rightarrow \mathcal{Y}^2$ and $W^+ : \mathcal{X} \rightarrow \mathcal{Y}^2 \times \mathcal{X}$ with transition probabilities

$$\begin{aligned} W^-(y_1 y_2 | x_1) &= \sum_{x_2 \in \mathcal{X}} \frac{1}{2} W(y_1 | x_1 \oplus x_2) W(y_2 | x_2), \\ W^+(y_1 y_2 x_1 | x_2) &= \frac{1}{2} W(y_1 | x_1 \oplus x_2) W(y_2 | x_2), \end{aligned} \tag{2}$$

where \oplus denotes mod-2 addition.

Notice that in an actual implementation of this transform one needs two independent copies of W to generate W^- and W^+ . In that sense, the transform preserves symmetric capacity,

$$I(W^-) + I(W^+) = 2I(W), \tag{3}$$

which is a direct consequence of the chain rule of mutual information. As for the other parameter, we have

$$\begin{aligned} Z(W^+) &= Z(W)^2 \\ Z(W) &\leq Z(W^-) \leq 2Z(W) - Z(W)^2 \end{aligned} \tag{4}$$

whose proofs can be found in [1]. Thus, the overall reliability is improved in the sense that

$$Z(W^-) + Z(W^+) \leq 2Z(W), \tag{5}$$

with W^+ more reliable than W and W^- less reliable than W .

B. Polarization process

Let (Ω, \mathcal{F}, P) be a probability space and suppose that $\{B_n : n = 1, 2, \dots\}$ is a sequence of i.i.d. random variables defined on this space with

$$P(B_1 = 0) = P(B_1 = 1) = \frac{1}{2}. \tag{6}$$

For $n \geq 1$, let \mathcal{F}_n be the σ -algebra generated by (B_1, \dots, B_n) . We may take $\mathcal{F} = \cup_{n=1}^{\infty} \mathcal{F}_n$.

Fix a channel $W \in \mathcal{W}$. Define a random sequence of channels $\{W_n \in \mathcal{W} : n \geq 0\}$ that starts at $W_0 = W$, and at time $n \geq 1$ sets

$$W_n = \begin{cases} W_{n-1}^- & \text{if } B_n = 1, \\ W_{n-1}^+ & \text{if } B_n = 0, \end{cases} \tag{7}$$

where the channels on the right side are defined by the transform $W_{n-1} \mapsto (W_{n-1}^-, W_{n-1}^+)$. Define two random processes $\{I_n : n = 0, 1, \dots\}$ and $\{Z_n : n = 0, 1, \dots\}$ by setting $I_n := I(W_n)$ and $Z_n := Z(W_n)$.

Observation 1:

- (i) $\{(I_n, \mathcal{F}_n)\}$ is a bounded martingale on $[0, 1]$ and converges a.s. to a r.v. I_∞ .
- (ii) $\{(Z_n, \mathcal{F}_n)\}$ is a bounded supermartingale on $[0, 1]$ and converges a.s. to a r.v. Z_∞ .

The martingale and supermartingale properties follow from (3), (5), and the convergence properties from general results on bounded martingales. It was shown in [1] and we will show in the sequel that the limit random variables I_∞ and Z_∞ are a.s. 0-1 valued. It then follows that $I_\infty + Z_\infty = 1$ in view of (1). Since $E[I_\infty] = I_0 = I(W)$, we have $P(I_\infty = 1) = I(W)$ and $P(I_\infty = 0) = 1 - I(W)$. Consequently $P(Z_\infty = 0) = I(W)$ and $P(Z_\infty = 1) = 1 - I(W)$. Thus the sequence of channels $\{W_n\}$ polarizes with probability one: they become perfect with probability $I(W)$, useless with probability $1 - I(W)$.

C. Polar coding

Channel polarization was used in [1] to develop a channel coding scheme called *polar coding*. Polar codes are a class of block codes with block-lengths constrained to $N = 2^n$, $n \geq 0$. These codes can be encoded in complexity $O(N \log N)$ and decoded by a successive cancellation decoder also in complexity $O(N \log N)$. These complexity bounds hold uniformly for all rates $R \in [0, 1]$, although for $R > I(W)$, they have no practical relevance.

To state the results precisely, let $P_e(N, R)$ denote the best achievable block error probability under successive cancellation decoding for polar coding with block length N and rate R . It was shown in [1] that for any given channel $W \in \mathcal{W}$, any n , and any $\gamma \in [0, 1]$, there exists a polar code with block-length $N = 2^n$, whose rate R and probability of block error under successive cancellation decoding P_e satisfy

$$R \geq P(Z_n \leq \gamma) \quad (8)$$

$$P_e \leq N\gamma. \quad (9)$$

The main result of [1] in this regard was to show that for any $R < I(W)$ the relation (8) can be satisfied for large N by taking the parameter γ as a function $\gamma(N, R) = o(N^{-\frac{5}{4}})$. This enabled [1] to conclude from (9) that $P_e(N, R) = o(N^{-\frac{1}{4}})$ for any fixed $R < I(W)$.

D. Summary of results

In this paper we improve the results of [1] by proving the following

Theorem 1: Let W be any B-DMC with $I(W) > 0$. Let $R < I(W)$ and $\beta < \frac{1}{2}$ be fixed. Then, for $N = 2^n$, $n \geq 0$, the best achievable block error probability for polar coding under successive cancellation decoding at block length N and rate R satisfies

$$P_e(N, R) = o(2^{-N^\beta}). \quad (10)$$

□

Remark 1: The bound (10) depends only on whether $R < I(W)$, but otherwise is not sensitive to R . Determining sharper

asymptotic results on $P_e(N, R)$ that display a more refined dependence on R remains a challenging open problem.

This result will follow from (8) and (9) as a corollary to the first half of the following

Theorem 2: Let W be any B-DMC. For any fixed $\beta < \frac{1}{2}$,

$$\liminf_{n \rightarrow \infty} P(Z_n \leq 2^{-N^\beta}) = I(W). \quad (11)$$

Conversely, if $I(W) < 1$, then for any fixed $\beta > \frac{1}{2}$,

$$\liminf_{n \rightarrow \infty} P(Z_n \geq 2^{-N^\beta}) = 1. \quad (12)$$

□

The rest of this paper is devoted to proving Theorem 2. The analysis will be carried out using the supermartingale $\{Z_n\}$. Section II abstracts out the general properties of this supermartingale so as to carry out the analysis in a more general framework unencumbered by the details of the original information-theoretic context. Theorem 2 is restated in Section II in a general setting and proved in the sections that follow. In Section V, we state some open problems.

II. PROBLEM RESTATEMENT

Let the probability space (Ω, \mathcal{F}, P) , the Bernoulli sequence $\{B_n : n = 1, 2, \dots\}$, and the σ -algebras $\{\mathcal{F}_n\}$ be defined in Section I-B above. We define the following class of random processes on (Ω, \mathcal{F}, P) .

Definition 1: For each $z_0 \in (0, 1)$, define \mathcal{Z}_{z_0} as the class of random processes $\{Z_n : n = 0, 1, \dots\}$ such that the process begins at $Z_0 = z_0$, Z_n is measurable with respect to \mathcal{F}_n , and follows trajectories satisfying

$$Z_{n+1} = Z_n^2 \quad \text{if } B_{n+1} = 1, \quad (13)$$

$$Z_{n+1} \in [Z_n, 2Z_n - Z_n^2] \quad \text{if } B_{n+1} = 0, \quad (14)$$

for $n \geq 0$. Let $\mathcal{Z} := \bigcup_{z_0 \in (0, 1)} \mathcal{Z}_{z_0}$.

The class \mathcal{Z} contains the processes $\{Z_n\}$ that were defined in Section I for all non-trivial channels $W \in \mathcal{W}$ for which $0 < Z(W) < 1$. The cases $z_0 = 0$ and $z_0 = 1$ are excluded from the definition since these lead to trivial processes which only complicate the statement of the results. Notice that the definition of \mathcal{Z} makes no reference to the information-theoretic origin of the problem, making the rest of the discussion fully self-contained.

Observation 2: For any $\{Z_n\} \in \mathcal{Z}$, the following hold.

- (i) $Z_n \in (0, 1)$ for all $n \geq 0$.
- (ii) $\{(Z_n, \mathcal{F}_n)\}$ is a bounded supermartingale.
- (iii) $\{Z_n\}$ converges a.s. and in \mathcal{L}^1 to a random variable Z_∞ , which is 0-1 valued a.s.

The first two observations are obvious. That $\{Z_n\}$ converges a.s. and in \mathcal{L}^1 is by general theorems on bounded supermartingales. Convergence in \mathcal{L}^1 implies that $E[|Z_{n+1} - Z_n|] \rightarrow 0$. But, $E[|Z_{n+1} - Z_n|] \geq (1/2)E[Z_n - Z_n^2] \geq 0$, which implies $E[Z_n(1 - Z_n)] \rightarrow 0$ and $E[Z_\infty(1 - Z_\infty)] = 0$. Thus Z_∞ equals 0 or 1 a.s.

We will prove Theorem 2 by proving the following equivalent

Theorem 3: For any $\{Z_n\} \in \mathcal{Z}$ and $\beta < \frac{1}{2}$, we have

$$\liminf_{n \rightarrow \infty} P(Z_n \leq 2^{-2^{\beta n}}) \geq P(Z_\infty = 0); \quad (15)$$

conversely, for $\beta > \frac{1}{2}$,

$$\liminf_{n \rightarrow \infty} P(Z_n \geq 2^{-2^{\beta n}}) = 1. \quad (16)$$

The proof of the converse part (16) will be given in the next section. The direct part (15) will be proved in Section IV.

III. PROOF OF THE CONVERSE PART

Fix a process $\{Z_n\} \in \mathcal{Z}$. Fix $\beta > 1/2$ and put $\delta_n(\beta) := 2^{-2^{\beta n}}$.

Let $\{\tilde{Z}_i\}$ be defined as the random process

$$\tilde{Z}_0 = Z_0, \quad \tilde{Z}_{i+1} = \begin{cases} \tilde{Z}_i^2 & \text{if } B_{i+1} = 1 \\ \tilde{Z}_i & \text{if } B_{i+1} = 0 \end{cases} \quad i \geq 0.$$

A comparison with (20) shows that $\{\tilde{Z}_i\}$ is dominated by $\{Z_i\} \in \mathcal{Z}$ and thus,

$$P(Z_n \geq \delta_n) \geq P(\tilde{Z}_n \geq \delta_n) \quad (17)$$

Notice that

$$\tilde{Z}_n = Z_0^{(2^L)} \quad (18)$$

with $L = \sum_{i=1}^n B_i$. Thus,

$$P(\tilde{Z}_n \geq \delta_n) = P(L + \log_2 \log_2(1/Z_0) \leq n\beta). \quad (19)$$

As $\beta > \frac{1}{2}$ and $Z_0 > 0$, by the law of large numbers, this probability goes to 1 as n increases, yielding (16).

IV. PROOF OF THE DIRECT PART

Definition 2: Given a process $\{Z_n\} \in \mathcal{Z}$ and a sequence of reals $\{f_n\} \subset [0, 1]$ convergent to 0, we will say that $\{f_n\}$ is *asymptotically dominating* (a.d.) for $\{Z_n\}$ and write $Z_n \prec f_n$ to mean that

$$\liminf_{n \rightarrow \infty} P(Z_n \leq f_n) \geq P(Z_\infty = 0).$$

We will say that $\{f_n\}$ is *universally dominating* (u.d.) for $\{Z_n\}$ if, for any fixed $k \geq 0$, the sequence $\{f_{n+k}\}$ is a.d. for $\{Z_n\}$.

In this notation, the direct part of Theorem 3 claims that, for $\beta < \frac{1}{2}$, the sequence $2^{-2^{\beta n}}$ is a.d. for every process in \mathcal{Z} . We will prove this claim in several steps. First, we define in Section IV-A a subclass of processes in \mathcal{Z} called *extremal processes*. Next, we show in Section IV-B that a sequence $\{f_n\}$ is a.d. for the class \mathcal{Z} if it is u.d. for the subclass of extremal processes. In Section IV-C, we show that $\{\rho^n\}$ with $\rho \in (\frac{3}{4}, 1)$ is a.d. for every extremal process. In Section IV-D, we use this result to show that, for any fixed $\beta < \frac{1}{2}$, the sequence $\{2^{-2^{n\beta}}\}$ is u.d. for extremal processes.

A. Extremal processes

Definition 3: A process $\{Z_n\} \in \mathcal{Z}$ is called *extremal* if

$$Z_{n+1} = \begin{cases} Z_n^2 & \text{if } B_{n+1} = 1, \\ 2Z_n - Z_n^2 & \text{if } B_{n+1} = 0. \end{cases} \quad (20)$$

The extremal process in \mathcal{Z}_{z_0} will be denoted by the notation $\{Z_n^{(z_0)}\}$ when we need to refer to it explicitly.

Note that the recursion for an extremal process can be written alternatively as

$$Z_{n+1} = Z_n^2 \quad \text{if } B_{n+1} = 1 \quad (21)$$

$$(1 - Z_{n+1}) = (1 - Z_n)^2 \quad \text{if } B_{n+1} = 0. \quad (22)$$

and also as

$$Z_{n+1} = Z_n + X_n Z_n (1 - Z_n), \quad n \geq 0 \quad (23)$$

where $X_n = (1 - 2B_n)$ is a ± 1 -valued random process. These forms emphasize the symmetric nature of the extremal process.

We state some properties of extremal processes that follow immediately from Observation 2.

Observation 3: For $\{Z_n\}$ any extremal process, in addition to Observation 2, we have

- (i) $\{Z_n\}$ is a Markov process.
- (ii) $\{Z_n\}$ is a bounded martingale.
- (iii) $P(Z_\infty = 0) = 1 - Z_0$, $P(Z_\infty = 1) = Z_0$.

The term *extremal* is justified by the following

Observation 4:

- (i) Every process $\{Z_n\} \in \mathcal{Z}_{z_0}$ is dominated by $\{Z_n^{(z_0)}\}$ on a sample function basis, i.e., $Z_n \leq Z_n^{(z_0)}$.
- (ii) The extremal process $\{Z_n^{(\alpha)}\}$ is dominated by $\{Z_n^{(\beta)}\}$ on a sample function basis for all $0 < \alpha \leq \beta < 1$.

B. A reduction argument

Proposition 1: If $\{f_n\}$ is a u.d. sequence over the class of extremal processes in \mathcal{Z} , then $\{f_n\}$ is a.d. over the class \mathcal{Z} .

Proof: Fix a process $\{Z_n\}$ in \mathcal{Z} and a sequence $\{f_n\}$ that is u.d. over the class of extremal processes. For any $k \geq 0$, $n \geq 0$, and $\delta \in (0, 1)$, we trivially have

$$P(Z_{k+n} \leq f_{k+n}) \geq P(Z_{k+n} \leq f_{k+n} \mid Z_k \leq \delta) P(Z_k \leq \delta). \quad (24)$$

Combining the observations

$$P(Z_{k+n} \leq f_{k+n} \mid Z_k \leq \delta) \geq P(Z_n^{(\delta)} \leq f_{k+n})$$

and

$$\liminf_{n \rightarrow \infty} P(Z_n^{(\delta)} \leq f_{n+k}) \geq (1 - \delta)$$

with (24), we see that for any fixed $k \geq 0$

$$\begin{aligned} \liminf_{n \rightarrow \infty} P(Z_n \leq f_n) &= \liminf_{n \rightarrow \infty} P(Z_{n+k} \leq f_{n+k}) \\ &\geq (1 - \delta) P(Z_k \leq \delta). \end{aligned}$$

Since this is true for all k , we obtain

$$\begin{aligned}\liminf_{n \rightarrow \infty} P(Z_n \leq f_n) &\geq (1 - \delta) \liminf_{k \rightarrow \infty} P(Z_k \leq \delta) \\ &\geq (1 - \delta) P(\liminf_{k \rightarrow \infty} Z_k \leq \delta) \\ &= (1 - \delta) P(Z_\infty = 0)\end{aligned}$$

where the second line follows by Fatou's lemma and the third by the a.s. convergence of $\{Z_k\}$ to the 0-1 valued Z_∞ . Letting $\delta \rightarrow 0^+$, we obtain

$$\liminf_{n \rightarrow \infty} P(Z_n \leq f_n) \geq P(Z_\infty = 0),$$

which completes the proof. \blacksquare

C. An asymptotically dominating sequence

Proposition 2: For any $\rho \in (\frac{3}{4}, 1)$, the sequence $\{\rho^n\}$ is a.d. over the class of extremal processes.

To prove this statement, let us fix $\{Z_n\}$ as an extremal process in \mathcal{Z} with $Z_0 = z_0$ for some $z_0 \in (0, 1)$.

Let $Q_n := Z_n(1 - Z_n)$. Then $Q_n \in (0, \frac{1}{4}]$ and

$$\begin{aligned}Q_{n+1} &= \begin{cases} Z_n^2(1 - Z_n^2) & \text{if } B_{n+1} = 1 \\ (2Z_n - Z_n^2)(1 - 2Z_n + Z_n^2) & \text{if } B_{n+1} = 0 \end{cases} \\ &= Q_n \cdot \begin{cases} Z_n(1 + Z_n) & \text{if } B_{n+1} = 1 \\ (1 - Z_n)(2 - Z_n) & \text{if } B_{n+1} = 0. \end{cases} \quad (25)\end{aligned}$$

Lemma 1 ([2]): $E[Q_n^{1/2}] \leq \frac{1}{2} \left(\frac{3}{4}\right)^{n/2}$.

Proof: Note that $\sqrt{z(1+z)} + \sqrt{(1-z)(2-z)} \leq \sqrt{3}$ when $z \in [0, 1]$. So, by (25), $E[Q_{n+1}^{1/2} | Q_n] \leq Q_n^{1/2} \left(\frac{3}{4}\right)^{1/2}$. Thus $E[Q_n^{1/2}] \leq E[Q_0^{1/2}] \left(\frac{3}{4}\right)^{n/2} \leq \frac{1}{2} \left(\frac{3}{4}\right)^{n/2}$. \blacksquare

By Markov's inequality, we obtain

Corollary 1: $P(Q_n \geq \rho^n) \leq \frac{1}{2} \left(\frac{3}{4\rho}\right)^{n/2}$ for $\rho > 0$.

We now turn this into a bound on Z_n .

Lemma 2: Let $f_n(\rho) := \frac{1 - \sqrt{1 - 4\rho^n}}{2}$ if $1 - 4\rho^n > 0$, $f_n(\rho) := 1$ otherwise. Then, $Z_n \prec f_n(\rho)$ for all $\rho \in (\frac{3}{4}, 1)$.

Proof: Fix $\rho \in (\frac{3}{4}, 1)$ and let $f_n = f_n(\rho)$. Note that for n large enough so that $1 - 4\rho^n > 0$, we have

$$\{Q_n \leq \rho^n\} = \{Z_n \leq f_n\} \cup \{Z_n \geq 1 - f_n\} \quad (26)$$

where the sets on the right side are disjoint. So, for n large enough

$$P(Q_n \leq \rho^n) = P(Z_n \leq f_n) + P(Z_n \geq 1 - f_n) \quad (27)$$

which gives

$$\begin{aligned}\liminf_{n \rightarrow \infty} P(Q_n \leq \rho^n) &\leq \liminf_{n \rightarrow \infty} P(Z_n \leq f_n) \\ &\quad + \limsup_{n \rightarrow \infty} P(Z_n \geq 1 - f_n).\end{aligned} \quad (28)$$

Since $\rho \geq \frac{3}{4}$, the left side of the above equation equals 1 by Corollary 1. Since f_n is monotonically decreasing,

$$\limsup_{n \rightarrow \infty} P(Z_n \geq 1 - f_n) \leq \limsup_{n \rightarrow \infty} P(Z_n \geq 1 - f_k) \quad (29)$$

for any $k \geq 1$. But $\limsup_{n \rightarrow \infty} P(Z_n \geq 1 - f_k) = z_0$. Thus,

$$\liminf_{n \rightarrow \infty} P(Z_n \leq f_n) \geq 1 - z_0, \quad (30)$$

which means that $Z_n \prec f_n$, as claimed. \blacksquare

The proof of Proposition 2 will be complete if we show that for every $\rho \in (\frac{3}{4}, 1)$, there exists $\tilde{\rho} \in (\frac{3}{4}, 1)$, such that $f_n(\tilde{\rho}) \leq \rho^n$ for all n large enough. It is easy to see that this is true for any $\frac{3}{4} < \tilde{\rho} < \rho$.

D. A bootstrapping argument

We now strengthen the result of the previous subsection and complete the proof of the direct part of Theorem 3.

Proposition 3: For any $\beta < \frac{1}{2}$, the sequence $\{2^{-2^{n\beta}}\}$ is u.d. over the class of extremal processes.

Proof: Fix $\beta < \frac{1}{2}$. First note that, for any fixed $k \geq 0$, asymptotically in n , we have $2^{-2^{(n+k)\beta}} = \Theta(2^{-2^{n\beta}})$ (using standard Landau notation). Hence, it suffices to prove that $\{2^{-2^{n\beta}}\}$ is an a.d. sequence.

Fix $\{Z_n\}$ as an extremal process. We wish to prove that $Z_n \prec 2^{-2^{n\beta}}$. Consider a second process $\{\tilde{Z}_i\}$ defined by fixing an $n \geq 1$ and an $m \in \{0, \dots, n\}$ and setting

$$\begin{aligned}\tilde{Z}_i &= Z_i, \quad i = 0, \dots, m, \\ \tilde{Z}_{i+1} &= \begin{cases} \tilde{Z}_i^2 & \text{if } B_{i+1} = 1 \\ 2\tilde{Z}_i & \text{if } B_{i+1} = 0 \end{cases}, \quad i \geq m.\end{aligned}$$

A comparison with (20) shows that $Z_i \leq \tilde{Z}_i$ for all $i \geq 1$.

Fix $a_n = \sqrt{n}$, and partition the set $\{m, \dots, n-1\}$ into $k = (n-m)/a_n$ consecutive intervals J_1, \dots, J_k of size a_n , i.e., $J_j = \{m + (j-1)a_n, \dots, m + ja_n - 1\}$. Let E_j be the event that $\sum_{i \in J_j} B_i < a_n \beta$. Observe that

$$P(E_j) \leq 2^{-a_n[1-\mathcal{H}(\beta)]} \quad (31)$$

where $\mathcal{H}(\beta) = -\beta \log_2(\beta) - (1-\beta) \log_2(1-\beta)$ is the binary entropy function. Thus the event $G := \cap_j E_j^c$ has probability at least $1 - k2^{-a_n[1-\mathcal{H}(\beta)]}$. Conditional on G , during every interval J_j the value of \tilde{Z} is squared at least $a_n \beta$ times and doubled at most $a_n(1 - \beta)$ times; hence, we have

$$\log_2 \tilde{Z}_{m+(j+1)a_n} \leq 2^{a_n \beta} [\log_2 \tilde{Z}_{m+ja_n} + a_n(1 - \beta)]$$

and so

$$\begin{aligned}\log_2 Z_n &\leq \log_2 \tilde{Z}_n \\ &\leq 2^{(n-m)\beta} \log_2 Z_m + a_n(1 - \beta) \sum_{j=1}^k 2^{ja_n \beta} \\ &\leq 2^{(n-m)\beta} \log_2 Z_m + a_n(1 - \beta) 2^{(n-m)\beta} (1 - 2^{-a_n \beta})^{-1} \\ &\leq 2^{(n-m)\beta} [\log_2 Z_m + a_n] \quad \text{for } n \text{ large enough.}\end{aligned}$$

Lastly, fix $m = n^{3/4}$, $\rho = 7/8$. Conditional on $\tilde{G} = \{Z_m \leq (\frac{7}{8})^m\} \cap G$ and for n large enough, we have $\log_2 Z_m \leq -n^{3/4} \log_2(8/7)$; hence,

$$\log_2 Z_n \leq 2^{(n-m)\beta} [-n^{3/4} \log_2(8/7) + n^{1/2}] \leq -2^{n\beta} o(1)$$

Noting that the probability of G approaches 1, we see by Lemma 2 that the probability of \tilde{G} approaches $1 - z_0$. This establishes that $Z_n \prec 2^{-2^{n\beta}}$ for any fixed $\beta < 1/2$. \blacksquare

V. OPEN PROBLEMS

Broadly stated, we have been interested in the asymptotic behavior of the cumulative probabilities $P(Z_n \leq z)$ for processes $\{Z_n\}$ derived from a channel polarization problem. The ultimate result in this regard would be to determine explicitly a function $E(n, R)$ such that, for any $R \in [0, 1]$,

$$\liminf_{n \rightarrow \infty} P(Z_n \leq 2^{-2^{E(n, R)}}) = R. \quad (32)$$

Theorem 3 gives only some partial characterization of $\frac{E(n, R)}{n}$ for large n .

The information-theoretic problem considered in this paper can be generalized in two main directions. First, one may consider the transform $W \mapsto (W^-, W^+)$ for channels with input alphabets $\mathcal{X} = \{1, \dots, q\}$ for arbitrary $q \geq 2$. In this generalization, the mod-2 addition operation \oplus may be replaced with addition mod- q , or even with an arbitrary group operation on \mathcal{X} . The process $\{I_n\}$ can be defined as before, the conservation law (3) still holds, and $\{I_n\}$ is a bounded martingale, which must converge a.s. An initial open problem for this case is to prove that channel polarization takes place, i.e., that $\{I_n\}$ converges a.s. to the set $\{0, \log_2 q\}$. Conditional on the validity of channel polarization, a subsequent goal would be to determine the rate of polarization.

Note that for $q \geq 3$, the auxiliary random process $\{Z_n\}$ can be defined only after giving a new definition for the channel parameter $Z(W)$. A natural definition is $Z(W) = \sum_{x \neq x'} \frac{1}{q(q-1)} \sum_y \sqrt{W(y|x)W(y|x')}$. Unfortunately, the relations (4) do not hold for this definition, and the process $\{Z_n\}$ does not appear likely to facilitate the analysis for $q \geq 3$.

A second direction for generalization of the problem is to consider more general channel transformations that preserve mutual information. For example, a ternary operation $W \mapsto (W', W'', W''')$ may be considered such that $I(W') + I(W'') + I(W''') = 3I(W)$. The random sequence of channels $\{W_n\}$ can be defined using a ternary fair coin, which ensures that $\{I_n\}$ is a bounded martingale. A major open problem in this general setting is to determine necessary and sufficient conditions on the channel transform to ensure channel polarization.

ACKNOWLEDGMENT

The authors wish to thank anonymous reviewers for their valuable comments and corrections on an earlier version of this manuscript. This work was supported in part by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under contracts no. 105E065 and 107E216.

REFERENCES

- [1] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," submitted to *IEEE Trans. Inform. Theory*, Oct. 2007. Online: <http://www.citebase.org/abstract?id=oai:arXiv.org:0807.3917>
- [2] B. Hajek, June 2007. Private communication.